Available online at www.sciencedirect.com
SCIENCE DIRECT®
Computational Geometry 33 (2006) 58–64
Computational Geometry
Theory and Applications
www.elsevier.com/locate/comgeo

Counterexamples to the uniformity conjecture

Daniel Richardson *,[1], Ahmed Elsonbaty [2]

Department of Computer Science, Bath University, Bath BA2 7AY, UK

Received 11 April 2003; accepted 20 February 2004

Available online 8 September 2005

Communicated by C. Yap and S. Pion

Abstract

The Exact Geometric Computing approach requires a zero test for numbers which are built up using standard operations starting with the natural numbers. The uniformity conjecture, part of an attempt to solve this problem, postulates a simple linear relationship between the syntactic length of expressions built up from the natural numbers using field operations, radicals and exponentials and logarithms, and the smallness of non zero complex numbers defined by such expressions. It is shown in this article that this conjecture is incorrect, and a technique is given for generating counterexamples. The technique may be useful to check other conjectured constructive root bounds of this kind. A revised form of the uniformity conjecture is proposed which avoids all the known counterexamples.

Keywords: Exact geometric computing; Uniformity conjecture; Witness conjecture; Diophantine approximation

1. Introduction

Attempts to bring the abstract notion of computation over the real and complex numbers as developed for example by Blum, Cucker, Shub and Smale [1], closer to the realities of numerical analysis and scientific computing are confronted with a basic problem: how to test whether or not a given number is equal to zero. Such a test is obviously part of the real number machine of Blum, Cucker, Shub and Smale, and is also to be found guarding most branch points of most algorithms in scientific computing. In particular, software developed within the Exact Geometric Computing framework (see [14]) requires a reliable evaluation of conditions which determine choice between alternative paths in an algorithm, and these conditions often involve a test for zero.

From this point of view, we need a theory of complexity of definitions of numbers which will tell us how small the absolute value of a defined non zero real or complex number can be in terms of the complexity of its definition. Such bounds are called constructive root bounds in the exact geometric computing literature (see [3,6,7,14]).

* Corresponding author.
E-mail address: masdr@bath.ac.uk (D. Richardson).
[1] Supported by the European RTN Network RAAG 2002-2006 (contract HPRN-CT-0027).
[2] Supported by the Egyptian government.

0925-7721/$ – see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.comgeo.2004.02.005

A classical bound of this type is the Liouville inequality, one form of which is given below. Suppose α is an algebraic number, and that the defining polynomial for α is $p(x) = a_0(x-\alpha_1)\dots(x-\alpha_d)$, where $p(x)$ has integral coefficients, and is irreducible. We define the Mahler measure of α to be

$$M(\alpha) := |a_0| \prod_{i=1}^{d} \max\bigl(1, |\alpha_i|\bigr).$$

For two algebraic numbers α and β, this gives a bound on $|\alpha-\beta|$ if $\alpha \neq \beta$. One form of this bound is:

$$2^{-rs} M(\alpha)^{-s} M(\beta)^{-r},$$

provided that α has degree r and β has degree s. Some computational experiments suggest that this bound is often too large. There is also some theoretical evidence for this. The Thue Siegel Roth theorem states that for any given algebraic number and any $\delta > 0$ there are only finitely many $p/q \in \mathbf{Q}$ so that $|\alpha - p/q| < q^{2+\delta}$. An improvement by Le Veque says that for any algebraic number field K, any algebraic number α, and $\delta > 0$ there are at most finitely many algebraic numbers $\beta \in K$ so that

$$|\alpha - \beta| < M(\beta)^{2+\delta}.$$

A symmetric form of the Thue Siegel Roth theorem has also been conjectured. This would say that for any number fields K_1 and K_2, and any $\delta > 0$ there are only finitely many α and β with $K_1 = \mathbf{Q}(\alpha)$, $K_2 = \mathbf{Q}(\beta)$, and

$$|\alpha - \beta| < \bigl(\max\bigl(M(\alpha), M(\beta)\bigr)\bigr)^{2+\delta}.$$

See [5] for discussion of all of the above, and further references.

It should be pointed out that there may be many zero tests within an algorithm, and in order to have software which is not too slow, it may be necessary to make use of number theoretic conjectures.

It seems that in order to improve the practical usefulness of the Liouville inequality, some other parameters ought to be considered, not only Mahler measure, height and degree. One possibility is to take the length of the defining expression into account.

The uniformity conjecture, discussed below, is a very general attempt to give such bounds in terms of the length. The conjecture has stood for several years. Counterexamples have recently been found however. A technique for generating such counterexamples is explained in the following section. This technique may also be useful for finding examples to check other conjectured constructive root bounds. In the last section a revised form of the uniformity conjecture is given which avoids all the known counterexamples.

2. The uniformity conjecture

The nested radical and exponential-logarithmic expressions are, roughly speaking, those which can be constructed from expressions for natural numbers using the operators $\{+, -, *, /, \sqrt[n]{\ }, \exp, \log\}$.

In the section below, the family of nested radical exponential-logarithmic expressions, (exp-log expressions for short), is described and the field of closed form numbers is defined. An expanded form is defined for the exp-log expressions, and the Uniformity Conjecture is stated. This claims that for expressions in expanded form, a small multiple of the syntactic length bounds the number of decimal places needed to distinguish the defined number from zero, if it is non-zero.

2.1. Expressions

We assume, to begin with, the usual canonical representation for the natural numbers base 10. Then the set of nested radical exponential and logarithmic expressions is the smallest set of expressions so that:

(1) All the canonical representations of natural numbers are in the set.
(2) If A and B are in the set so are $(A+B)$, $(A-B)$, and $(A*B)$, (A/B).
(3) If A is in the set, so are $-A$, $\exp(A)$ and $\log(A)$.
(4) If A is in the set and n is a canonical representation of a natural number bigger than 1, then $A^{1/n}$ is in the set.

Each nested radical exponential and logarithmic expression E is either undefined, or is interpreted as a real or complex number $V(E)$, as follows.

(1) If E is a representation of an natural number, $V(E)$ is that natural number.
(2) The operators are given the usual precedence in the absence of brackets.
(3) If A and B are defined, then $V(A+B)$, $V(A-B)$, $V(A*B)$ and $V(-A)$ are defined with the usual interpretation of the operators. If B is defined, and $V(B)$ is not zero, then $V(A/B)$ is defined, with the usual interpretation.
(4) If A is defined, then $\exp(A)$ is defined with meaning e^A.
(5) If A is defined, and $V(A) \neq 0$, then $\log(A)$ is defined, as the branch of the logarithm base e so that $-\pi < \mathrm{Im}(\log(A)) \leqslant \pi$.
(6) If A is defined and $V(A) \neq 0$, and n is a canonical representation of a natural number bigger than 1, then $A^{1/n}$ is defined and equal to $\exp(\log(A)/n)$.

The operator V is called evaluation.

The complex numbers defined in this way are called *closed form numbers* [4]. The complex number i is a closed form number. The closed form numbers are closed under trigonometric functions, expressed in terms of the exponential function, and their inverses, expressed in terms of logarithms. All these functions are useful in geometric computing.

A field with good closure properties including the closed form numbers is the field of elementary numbers. These are numbers of the form $q(\alpha)$, where q is in $\mathbf{Q}[x_1, \ldots, x_n]$, and $\alpha \in \mathbf{C}^n$ is a non singular solution of a system of equations $(p_1, \ldots, p_n) = 0$ and each p_i is in $\mathbf{Z}[x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n}]$. It has been shown that this is an effective field, i.e., equality is decidable if the Schanuel conjecture is true. See [8,9].

Please notice that although we have expressions here for nth roots, we do not have expressions for nth powers. If we want A^2, for example, we have to write it as $A * A$.

2.2. Length of an expression

We define the length of a natural number to be the number of digits base 10 which are used to represent it in the usual canonical form.

Each exp-log expression may be considered as a tree with representations of natural numbers on the frontier and operators among $\{+, -, *, /, \sqrt[n]{\ }, \exp, \log\}$ on the interior nodes. We allow – to have arity either 1 or 2. The radical sign has arity 2, and its first argument must be a natural number in canonical form. We define the length of an expression to be the sum of the number of interior nodes, i.e., the number of operators, and the sum of the lengths of the representations of natural numbers on the frontier. We use length(E) to denote the length of expression E. So, for example, in decimal notation, $4 - 3 * (10)^{1/8}$ would have length 8, since it has 5 digits and 3 operator symbols.

2.3. Gap functions

Definition 1. A gap function for the closed form numbers is a function $g : Exp \to \mathbf{R}_+$, where *Exp* is the set of nested radical exponential and logarithmic expressions, so that if x is a closed form number represented by an expression A, and $x \neq 0$ then $|x| > 10^{-g(A)}$.

Several different groups of people have worked with this idea, using different terminology. A gap function is essentially the same as a constructive root bound.

A gap function tells us the amount of decimal precision which is needed to distinguish a non-zero number from zero. Of course gap functions exist. We hope that there is a computable gap function, and even an easily computable gap function.

An important question is: How does the evaluation operator, V, behave with respect to the two natural measures we have namely, the length of an expression and the logarithm of the absolute value of complex numbers? For some more discussion of this question, (with a slightly different definition of length) one can refer to [10].

2.4. Uniformity conjecture

Definition 2. We consider an expression E to be a subexpression of itself. We will say that an expression E is in expanded form if for any exponential subexpression $\exp(A)$ of E, we have $|V(A)| \leqslant 1$.

Uniformity Conjecture. *If E is an expression in expanded form, and $V(E) \neq 0$, then $|V(E)|$ is bigger than 10^{-2k}, where k is the length of E.*

Note that this would allow fairly quick zero recognition for numbers defined by radicals. This is certainly a desirable goal.

The witness conjectures of Joris Van Der Hoeven are related to this. These postulate various relationships between length of expression and number of digits needed to distinguish the defined number from zero, if it is non-zero. See [11–13].

An example is $3 * \log(640320)/\sqrt{163} - \pi$ which, although famous for being small, is only zero to 15 decimal places, whereas its syntactic length is 15 plus the length of π. We can replace π with $\log(-1)/\sqrt{-1}$ with length 8.

3. Counterexamples

A number of computationally intense searches for counterexamples failed to find any. We know as a result of these searches, for example, that there are no counterexamples of length less than 8. The counterexamples began to be discovered quite recently in the following way. David Bailey suggested that we look at Borwein's fourth order approximation method for π. See [2].

$$y_0 = \sqrt{2} - 1, \quad x_0 = 6 - 4\sqrt{2}$$
$$y_n = \bigl(1 - (1 - y_{n-1}^4)^{1/4}\bigr)/\bigl(1 + (1 - y_{n-1}^4)^{1/4}\bigr),$$
$$x_n = (1 + y_n)^4 x_{n-1} - 2^{2n+1} y_n (1 + y_n + y_n^2)$$

with x_n tending to $1/\pi$ as $n \to \infty$.

After 15 iterations, this produces an approximation with billions of digits of accuracy. By substituting the recurrence relation into itself a number of times, expressions can be found for the approximation. This was quite a helpful idea, but it did not seem to produce a counterexample. The reason was that although the precision grows by a factor of four at each substitution, the length of the approximating expression grows even faster.

If $E(x)$ is some expression with k occurrences of x in it, then $E(E(x))$ has k^2 occurrences of x in it. In general if we define $E_1(x) = E(x)$, and $E_{n+1}(x) = E_n(E(x))$, then $E_n(x)$ will have k^n occurrences of x in it, and the length of $E_n(x)$ grows like k^n. On the other hand, we observe that if $E(x)$ has a zero at zero of multiplicity m, then $E_n(x) = \mathrm{O}(x^{m^n})$. So to get a counterexample we would require $k < m$. At this point Joris Van Der Hoeven produced the first counterexample generator:

$$E(x) = \log(1 + x) - 2\log\left(1 + \log\left(1 + \frac{x}{2}\right)\right).$$

This has only two occurrences of x, but is $\mathrm{O}(x^3)$ at zero. More precisely, $E(x) = x^3/24 + \mathrm{O}(x^4)$ at values of x near zero. The third derivative of $E(x)$ is less than 1 for all x with absolute value below $1/10$. This means that if $x = 10^{-N}$, then $E_n(x)$ has length approximately $2^n N$, but $|E_n(x)|$ is below $10^{-3^n N}$, provided $N > 1$.

The length of $E(x)$ is $2\,\mathrm{length}(x) + 14$. Let $x = 10^{-N}$. Since the length of x is $N + 3$, the length of $E_2(x)$ is $4N + 54$. So choosing $N = 109$ gives a counterexample. In fact $|E_2(10^{-109})| < 10^{-986}$. On the other hand $2\,\mathrm{length}(E_2(10^{-109})) \leqslant 980$. This can seemingly be verified in any computer algebra system (for example, in Maple or Reduce) using 1000 digits of precision. As pointed out by a referee of this paper, however, although these systems attempt to return full precision accuracy they do not guarantee this. This remains a problem even if we increase the number of digits of precision to, for example, 10,000. In this case, however, we can verify the fact that this is a counterexample by some analysis, as follows. We find $E'''(x)$ symbolically. This turns out to be the sum of four terms with small integers in the numerators, and with denominators which are easy to estimate for x in the interval $[0, 1/10]$. In this way we find that $E'''(x)$ has absolute value less than 1 in this interval, as mentioned above. From this we find

that, for each x in this interval, $E(x) = (d_3/6)x^3$, for some number d_3 with absolute value less than 1, depending on x. From this it follows that $E_2(x) = cx^9$ for some number c with absolute value less than 1. And therefore we must have $|E_2(10^{-109})| < 10^{981}$.

3.1. More counterexamples

We have also constructed more counterexamples with logarithms, exponentials, and radicals. An example is

$$F(x) = (1+x)^{1/2} - 2(1+3x/4)^{1/3} + 1.$$

$F(x)$ is, again, $O(x^3)$ at zero. More precisely, $F(x) = x^3/96 + O(x^4)$ for x near zero. The length of $F(x)$ is $2\,\text{length}(x) + 17$. Suppose $x = 10^{-N}$. The length of x is then $N+3$. Thus $\text{length}(F(10^{-N})) = 2N + 23$. On the other hand $|F(x)| < 10^{-3N}$ for x near zero. We do not yet get a counterexample however because of the factor of 2 in the exponent of the conjecture.

However, $|F(F(x))| \leqslant x^9$ for x near zero. So a counterexample is obtained by choosing N sufficiently large and substituting $x = 10^{-N}$ into $F(F(x))$. In this case

$$\left|F\left(F(10^{-126})\right)\right| < 10^{-1141} \quad \text{and} \quad 2\ \text{length}\left(F\left(F(10^{-126})\right)\right) \leqslant 1134.$$

As before, this can seemingly be directly verified in any computer algebra system, using sufficiently high precision. It can actually be verified in a system with guaranteed precision. The fact that this is a counterexample can also be verified by hand, using the same simple pattern of analysis as above.

Define $F_1(x) = F(x)$ and $F_{n+1}(x) = F_n(F(x))$. Then, assuming $x = 10^{-N}$ we get

$$\text{length}\left(F_n(x)\right) = O(2^n) \quad \text{and} \quad \left|F_n(x)\right| = O(x^{3^n}).$$

There are even worse examples, also with two occurrences of x. Let

$$G(x) = \sqrt{1+x} - \frac{25}{4} + \frac{21}{4}\sqrt{\frac{7}{5} - \frac{2}{5}\sqrt{-7 + 8\sqrt{1+\frac{5}{21}x}}}.$$

$G(x) = O(x^5)$ near zero. In this case we could get a counterexample from $G(x)$ with $x = 10^{-N}$ and N sufficiently large.

The method we have used for searching for such functions is the following. We take any exp-log function $f(x)$ with $f(0) = 0$, and such that $f(x)$ has an expression representing it in which there is only one occurrence of x. Set

$$h_1(x) = a_1 f(a_0 x),$$
$$h_{k+1}(x) = a_{k+1} f\left(h_k(x)\right) \quad \text{for } k = 1, \ldots, n-1,$$

so that

$$h_n(x) = a_n f\left(a_{n-1} f\left(\ldots a_1 f(a_0 x)\right)\ldots\right)$$

and let

$$g_n(x) = f(x) - h_n(x).$$

In the expression for $g_n(x)$ there are two occurrences of x, and there are $n+1$ parameters $a_0, \ldots, a_n$. We have $g_n(0) = 0$ since $f(0) = 0$. We now try to find values of the parameters so that $g_n(x)$ is $O(x^{n+1})$ at the origin, but $g_n(x)$ is not identically zero. This involves solving n polynomial equations in $n+1$ unknowns. If there is a solution, there is a solution which is algebraic in the coefficients of the Taylor series for $f(x)$, since the equations are polynomial in these coefficients. In order to construct a counterexample, we also require that the parameters in the solution are closed form numbers. In practice this means that we look for solutions which can be constructed by nested radicals from the Taylor coefficients of $f(x)$. A problem with the construction is that as soon as one parameter takes the value zero then $h_n(x)$ is identically zero.

Suppose we take $f(x) = (x+1)^{1/r} - 1$. In this case we can find values of the parameters represented by radicals, depending on r, so that $g_n(x) = O(x^{n+1})$ at the origin, for $n = 1, 2, 3, 4$. In some cases, we found solutions which

were rational, depending on r, and in other cases the solutions required use of radicals, or imaginary numbers. We were not able to solve the equations, or even to decide whether or not they have a solution, in any case with $n > 4$.

Here are two more examples with different base functions:

$$\ln(1+x) + 3\ln\left(1 - \frac{1}{2}\ln\left(1 + \ln\left(1 + \frac{2}{3}x\right)\right)\right) = -\frac{1}{1215}x^5 + \mathrm{O}(x^6), \tag{1}$$

$$\frac{3}{2}\exp\left(\exp\left(-2\exp\left(-\frac{1}{3}x\right) + 2\right) - 1\right) - \frac{1}{2} - \exp(x) = -\frac{1}{1215}x^5 + \mathrm{O}(x^6). \tag{2}$$

Using similar methods, we can construct examples based on $\sin(x)$, although in this case the original exp-log expression has two occurrences of x rather than just one, and the result, as an exp-log expression, has four occurrences of x. For example,

$$2\sin\left(\frac{1}{3}\sqrt{3}\sin\left(\frac{1}{2}\sqrt{3}x\right)\right) - \sin(x) = \frac{1}{80}x^5 + \mathrm{O}(x^6).$$

4. Revised uniformity conjecture

The method of constructing counterexamples explained above involves finding expressions $g_n(x)$ with only two occurrences of x but so that $g_n(x) = \mathrm{O}(x^{n+1})$ at zero. Once we have such an expression, we define $E_k(x)$ to be an expression representing the kth iterate of $g_n(x)$. Such $E_k(x)$ would have length $\mathrm{O}(2^k)$, and the resulting function would be $\mathrm{O}(x^{(n+1)^k})$ at the origin. We only succeeded in solving the related sets of equations up to $n = 4$.

All of the examples we have constructed involve fairly deep nesting, which can be defined as follows. We will say that the depth of a canonically expressed natural number is 1. Also let the depth of $A + B$, $A - B$, $A * B$, A/B be one plus the maximum of the depths of A and B. Let $\mathrm{depth}(\log(A)) = \mathrm{depth}(\exp(A)) = \mathrm{depth}(A^{1/n}) = \mathrm{depth}(A) + 1$. The idea is that the depth of an expression is the number of nodes in the longest path in the expression tree.

We note that, in our examples, the depth of $g_n(x)$ increases linearly with n, and the depth of $E_k(x)$ increases linearly with k.

We also define the height H of an expression to be the maximum of the absolute values of the integers which occur in the expression.

Revised Uniformity Conjecture. *If E is an expression in expanded form, and $V(E) \neq 0$, then $|V(E)|$ is bigger than $\max(H, 2)^{-C2^d}$, where H is the height of E, d is the depth of E, and C is a universal constant independent of E.*

Even with $C = 1$, we have not been able to find any counterexamples. As an example, and taking $C = 1$, this would give a bound of H^{-8} for $|2^{1/n} - p/q|$, where H is a bound on $n, |p|, |q|$. So, in case n is large, this gives something stronger than the Liouville inequality stated above, but not as strong as might be suggested by the Thue Siegel Roth theorem.

References

[1] Blum, Cucker, Shub, Smale, Complexity and Real Computation, Springer.

[2] J.M. Borwein, P.B. Borwein, Pi and the AGM, John Wiley, Canadian Mathematical Society, 1987.

[3] C. Burnikle, S. Funke, K. Mehlhorn, S. Schirra, S. Schmitt, A separation bound for real algebraic expressions, in: Lecture Notes in Computer Sci., Springer, Berlin, 2001, pp. 254–265.

[4] T.Y. Chow, What is a closed-form number?, Amer. Math. Monthly 106 (5) (1999) 440–448.

[5] J.H. Evertse, Symmetric improvements of Liouville's inequality: A survey, in: F. Halter-Koch, R.F. Tichy (Eds.), Algebraic Number Theory and Diophantine Analysis, Proc. Conf. Graz 1998, Walter de Gruyter, 2000, pp. 129–141.

[6] C. Li, Exact geometric computation: Theory and applications, Ph.D. Thesis, Department of Computer Science, New York University, 2001.

[7] C. Li, C. Yap, A new constructive root bound for algebraic expressions, in: 12th ACM-SIAM Symp. on Discrete Algorithms, Jan. 2001, pp. 496–505.

[8] D. Richardson, How to recognise zero, J. Symbolic Comput. 24 (1997) 627–645.

[9] D. Richardson, Multiplicative independence of algebraic numbers and expressions, J. Pure Appl. Algebra 164 (2001) 231–245.

[10] D. Richardson, The uniformity conjecture, in: Proceedings of Computability and Complexity in Analysis, CCA2000, Swansea, Wales, in: Lecture Notes in Comput. Sci., vol. 2064, Springer, Berlin, 2001, pp. 253–272.

[11] J. Van Der Hoeven, Automatic numerical expansions, in: J.-C. Bajard, D. Michelucci, J.-M. Moreau, J.-M. Muller (Eds.), Proc. of the Conference "Real Numbers and Computers", Saint-Etienne, France, 1995, pp. 261–274.
[12] J. Van Der Hoeven, Automatic asymptotics, Ph.D. Thesis, Ecole Polytechnique, 1997.
[13] J. Van Der Hoeven, Zero-testing, witness conjectures and differential diophantine approximation, Preprint.
[14] C.K. Yap, Robust geometric computation, in: J.E. Goodman, J. O'Rourke (Eds.), Handbook of Discrete and Computational Geometry, second ed., Chapman & Hall/CRC, Boca Raton, FL, 2004, pp. 927–952.

Further reading

[15] A. Baker, Transcendental Number Theory, CUP, 1975.
[16] J.M. Borwein, P.B. Borwein, On the complexity of familiar functions and numbers, SIAM Rev. 30 (4) (1988) 589–601.
[17] S. Lang, Introduction to Transcendental Numbers, Addison-Wesley, 1966.
[18] D. Richardson, A. Elsonbaty, Use of algebraically independent numbers for zero recognition of polynomial terms, J. Complexity 19 (2003) 631–637.
[19] C.K. Yap, Fundamental Problems of Algorithmic Algebra, Oxford University Press, Oxford, 2000.